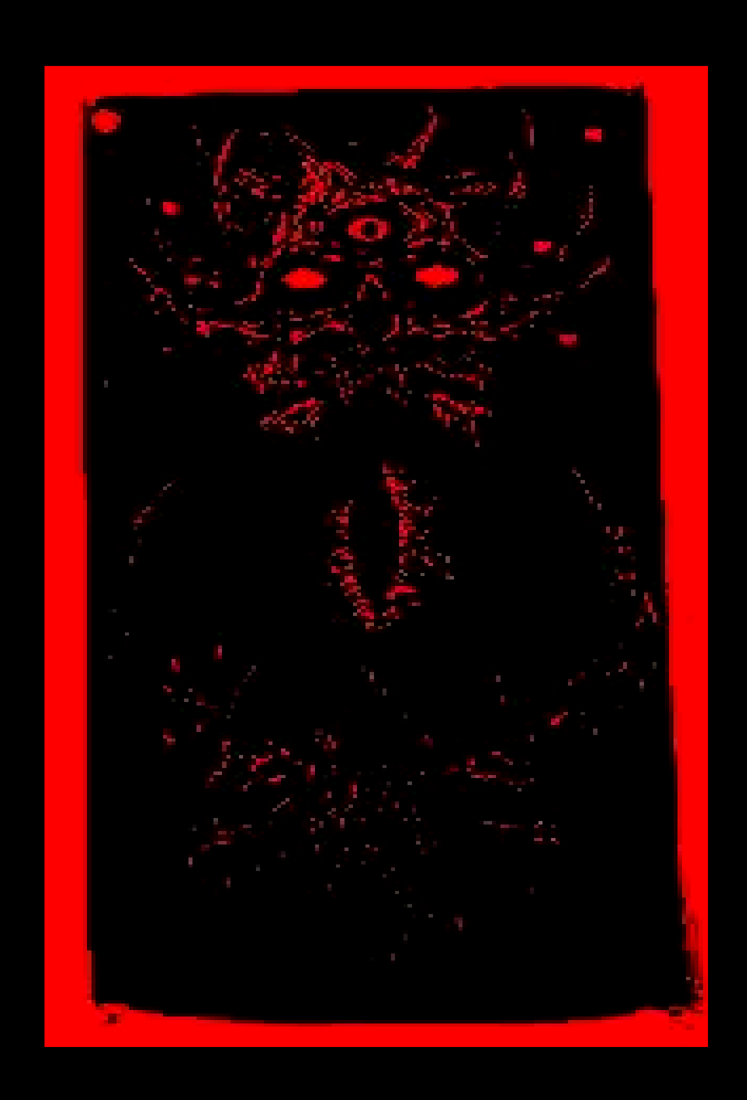
"OCULTO"

ILLEGALISMO CRIPTATO EGOICO



NECHAYEVSHCHINAED

“OCULTO”

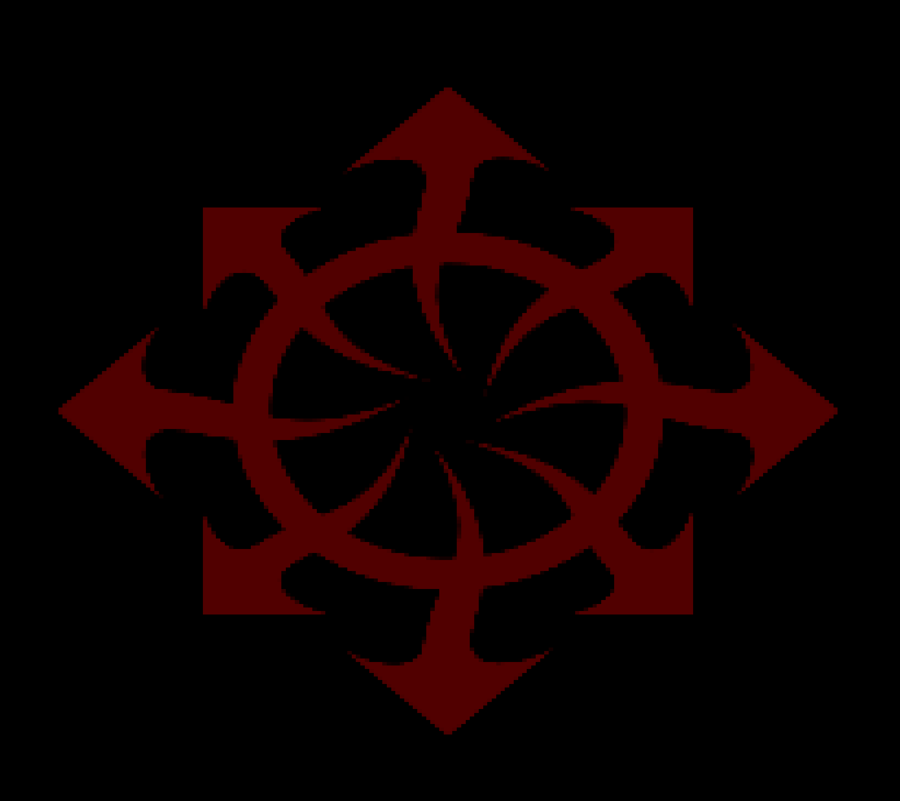
INDICE

ANONIMATO

CIFRADO

SEGURIDAD MÓVIL

- **CORREOS CIFRADOS**
- **ENCRIPTAR DIRECTORIO**
- **APLICACIONES VARIAS**



NECHAYEVSHCHINAED@PROTONMAIL.COM

INTRO

TERRORISTICO

ILLEGALE

Espropriando la Prima Presente parte, porto avanti il "Progetto Ilegalista", che si estende ai codici criptati per Avanzare in una società di zombie ambulanti. Vado subito al dunque- il tempo "non esistente" non permette di aspettare chicchessia -e Affermo che l'uso del criptato è unito- e mai diviso- nelle varie forme di illegalismo scelte per il godimento dell'Individuo Nichilista!
Criptato Illegalista che conduce a una seria riflessione - ma che sarà sprofondata in altro modo- sulla clandestinità(o latitanza per dirlo in gergo anti giuridico e di riflesso giuridico) per Colpire il sacro altare del bene e del male.
Nel presente panfleto sono presentati vari metodi di crittazione o di anonimato per sfuggire alla rete societaria di eguaglianza(cani da guardia e onesti cittadini), ma come si può sfuggire alla normalità di presentare un documento di identità nominalmente vero?
La clandestinità unita all'uso del crittato per continuare il proprio Progetto Ilegalista, è una vita che ricerca il margine, per spezzarlo,e Annientare il diritto all'esistenza.

Al Presente questo nuova uscita editoriale della Terroristica e Nichilistica -NECHAYEVSHCHINAED- va allo scontro contro il "reale", il volto del bene contro quello del male(e di una Cattiva Passione), all'uso dell'esplosivo, della pistola,e della Parola Affilata come un rasoio che taglia le carni malate dell'eguaglianza.

Il Nichilismo Terrorista di cui sono fautore si fonde con l'Indiscriminazione, la ricerca dell'Obiettivo Egoico e specifico, contro il soliloquio di innocenti blog, che muoiono di noia,mentre aspettano il prossimo Attentato, che li porti a pensare cosa "pubblicare", senza cadere in una scusa retorica,tanto vuota di Dibattito!
A loro dico: Prendere o lasciare!
Per il Terrorismo Nichilista e Indiscriminato!
Per l'uso del Criptato in una vita illegale!
Affinità Egoista nelle strade polverose delle metropoli,a Frenitida!


"ANONIMATO"

TOR

Tor es el programa más conocido para el anonimato en la red... Tiene algo bueno y es que está diseñado por activistas y dirigido a activistas, por lo que nos da la seguridad de que nos ponemos en las manos de gente que está por lo mismo que nosotras.

Pero, aunque como hemos dicho tiene cosas buenas, también tiene otras, no tan buenas (para una servidora que por supuesto nadie tiene que coincidir con esta opinión). No es muy rápido y si lo que queréis es hackear, ya sea inyecciones SQL, hacer ataques DDOS o lo que os dé la gana, con esta herramienta estáis bastante limitadas y yo no aconsejaría usarla para esos fines, ya que Tor crea una navegación anónima del buscador, pero no del ordenador en sí mismo.

Pero para lo que se diseñó, tal como hacer búsquedas en internet de manera segura. Lo hace muy bien.

Tor está diseñado para incrementar el anonimato de tus actividades en Internet. Este disfraza tu identidad y protege tus actividades en línea de las diversas formas de vigilancia en la red. También puede ser utilizado para eludir los filtros en Internet. Es de código abierto y software Libre, así que no estaremos colaborando con corporaciones.

Para su instalación en Linux. Lo podemos encontrar para descargar en https://www.torproject.org/download/download-easy.html.en

Seleccionamos el idioma que queramos y descargamos

el paquete de *Tor Browser Bundle for GNU/Linux*. Habremos descargado un archivo .tar.gz, que una vez descargado lo guardaremos donde queramos y lo abriremos cuando necesitemos.

Este paquete que habréis descargado es un portable con lo que nos ahorra instalaciones, facilitando su uso.

Para ejecutarlo deberemos ir al directorio donde lo guardamos, lo descomprimiremos y únicamente tendremos que presionar sobre el icono que dice: *start-tor-browser*

Cuando hagáis clic encima del archivo aparecerá una ventana donde el programa solo, intentará conectarse a la red Tor.

Cuando haya terminado se abrirá un Firefox anónimo donde trabajaremos con Tor. A parte de este firefox, si lo deseamos, podemos abrir nuestro propio Mozilla para trabajar más rápido, pero teniendo en cuenta que este no será tan fiable como el de la red Tor.

La facilidad de esta herramienta junto al buen resultado que ofrece, son buenos motivos para usarlo, siempre y cuando respetemos lo que anteriormente comentábamos acerca de los usos que le queramos dar.

Para la instalación en Windows el proceso es el mismo.

Entramos en el mismo enlace de descarga, pero esta vez descargaremos el paquete destinado a la distribución de Windows. Una vez descargado el paquete, hay que

hacer clic encima de este y el resultado de la extracción será una carpeta donde habrá un .exe que será la aplicación.

Durante estos últimos años Tor ha hecho un gran trabajo de configuración ya que anteriormente había que hacer la instalación de tres paquetes para poder navegar con él, mientras que con este programa portable, no hace falta ninguna instalación.

Además de que el uso del proxy (más adelante veremos qué es un proxy) de Tor es utilizado por otros programas destinados a la navegación anónima, como por ejemplo

Proxychains, que está disponible para Linux únicamente y del que a continuación veremos cómo funciona.


TAILS

Recién acabamos de hablar de Tor. Ahora nos toca hablar de Tails, un Live CD que como veréis tiene bastante que ver con el anterior software.

Tails es un Live CD aislado que se encargará de conectarse anónimamente a la red, y lo hará desde la red Tor. Una de las características de Tails es que trabaja sin dejar rastro, a menos que se indique explícitamente, en los discos duros que puedan haber en el ordenador donde se introduzca. ¿El motivo? Poder trabajar en un entorno seguro en el que la conexión sea lo más privada y anónima posible. Otra de las ventajas de Tails es que está basado en Debian GNU/Linux, pero a la hora de empezar a trabajar con el Live CD, os pedirá si queréis trabajar en el entorno camuflado de Windows XP, con lo que una vez seleccionada esta opción, tanto el fondo de escritorio como el entorno, son idénticos a XP. Y tal como explican en su página web, uno de los motivos por los que se creó Tails, es para trabajar en un local comercial, por ejemplo un locutorio de internet, y con el entorno creado por Tails nadie distingue si se está trabajando con un Live CD o con el mismo sistema del propio local, apartando así, cualquier sospecha de personas que pasen a vuestro lado.

Además de que Tails, no dejará ningún rastro en el ordenador anfitrión de que se ha trabajado con otro sistema.

Y por si esto fuera poco, Tails tiene otras herramientas de seguridad, como LUKS, el estándar de Linux para cifrar USB o discos duros. Cifra las conexiones con HTTPS, tiene en su software aplicaciones de correo o mensajería instantánea en las que se puede usar complementos de cifrado como OpenPGP o OTR (Off The Record) respectivamente. Además de que cuenta con Nautilus Wipe para el borrado y sobreescritura de archivos.

Hay algo que cualquiera que use Tails deberá saber. Cuando navegamos con Tails, estamos navegando en la red Tor, a no ser que no queramos. De este modo la conexión es semianónima, pero el rastro que dejamos en la red muestra que estamos usando Tails, e incluso que estamos usando Tor. Este concepto no es que sea negativo, pero sí algo a tener en cuenta.

Algo que para algunas de nosotras sí es algo negativo, o por lo menos a tener muy pero que muy en cuenta, es que en Tails colaboran varios proyectos entre los cuales está Lightweight Portable Security (LPS). Este programa que colabora con Tails es un

programa realizado por el Laboratorio de la Fuerza Aérea de Investigación, Anti-Sabotaje - Iniciativa de Protección de Software (ATSPI) Oficina de Tecnología, creado para proteger la propiedad intelectual (software de aplicación), de la piratería, el sabotaje y las amenazas contra el estado americano.

A quien le dé un poco de grima esto, mejor busque alternativas para trabajar de esta forma, aunque hay que tener en cuenta que casi todo el mundo usa Windows, y pocos software colaboran tanto con las autoridades como él, aunque usar una distribución que directamente colabora con un proyecto como ese no apetece mucho, verdad? La verdad es que es un buen software. Que cada una haga lo que crea necesario...

También Tails forma parte del proyecto de Ubuntu Privacy Remix (UPR), del que hablaremos más adelante, y del que no puedo confirmarlo, pero espero que no colabore con LPS yaque como se mostrará en el capítulo dedicado a UPR, es el mejor método para manejar información realmente sensible, y si LPS estuviera en medio de UPR, generaría sospechas acerca de la seguridad y eficacia de Ubuntu Privacy Remix.

Como alternativa a Tails, existe “AnonymO.S. Live CD”, que funciona de la misma manera que Tails, navegando a través de Tor, cambiando si queremos la dirección MAC (una especie de código de serie, único, de cada red), incluso podemos usarlo con el entorno de Windows XP.

A continuación seguirá una pequeña guía de Tails para hacer un primer y básico uso de esta distribución, mostrando de manera sencilla (lo más sencilla que podamos) como conectarse a la red o enviar un comunicado (por ejemplo).

Para más información sobre Tails, así como para descargarlo deberéis entrar en https://tails.boum.org/.

Para empezar a trabajar con este Live CD, deberemos introducir el DVD/CD o el USB booteable con Tails, reiniciamos el ordenador y deberemos entrar en la BIOS del ordenador, para a continuación seleccionar el arranque desde el dispositivo que contenga Tails (esto depende del ordenador, pero a no ser que este sea muy antiguo podréis hacerlo sin problemas). Una vez el software ha empezado el arranque, aparecerá una pantalla donde en el panel inferior podremos cambiar el idioma a aquel que deseemos. Con el idioma cambiado debe-

remos escoger si queremos que el programa nos muestre más opciones o que arranque ya mismo. Escogeremos la opción de *Más opciones*. Aparecerá una nueva ventana y en ella deberemos decidir una contraseña para poder trabajar como root y así poder configurar más herramientas de Tails tales como el uso o desuso de los discos duros del ordenador, o la configuración de llaves para encriptar. En esta misma ventana marcaremos la casilla *Activar camuflaje de Microsoft Windows XP*.

Una vez Tails ya está corriendo y de pronto parece que estemos trabajando en una máquina con XP esperaremos un rato que vaya cargando (hay que tener en cuenta que si lo hemos cargado en un DVD/CD o un USB irá más lento) y aparecerá la ventana principal de Iceweasel, que es el navegador por defecto y con el que trabajaremos de forma anónima a través de la red Tor. En el caso de que no apareciera deberíamos ir a *Start – Internet – Iceweasel* y ya estaríamos navegando con Tor.

Como ejemplo para este primer inicio con Tails vamos a imaginar que queremos mandar un comunicado de una acción o una convocatoria cualquiera y que la información de esta la tenemos guardada en un archivo de texto dentro de un USB (ahora

mismo da igual que esté encriptado el USB, el texto o que no lo estén), hemos ido a un locutorio de internet, hemos puesto el Live CD de Tails y hemos arrancado en modo camuflaje Windows XP, con lo que estamos pasando desapercibidas en un ordenador cualquiera de los que hay.

Una vez hecho estos pasos anteriores, a continuación deberemos dirigirnos a *Start – Lugares – My computer* y en la ventana que aparece seleccionaremos el dispositivo donde se encuentre el texto, lo buscaremos, abriremos y lo mandaremos donde queramos como si hubiéramos estado en nuestra casa haciendo esto (esto último por favor no lo hagáis nunca). Lo mejor de todo es que no habremos dejado ningún rastro (más que en las posibles cámaras que hubieran en el local) en esa máquina, salvo en la memoria RAM (esta se eliminará en el momento de apagar el ordenador o cerrar Tails). Si hemos trabajado en modo XP no aparecerá, pero si hemos trabajado desde el entorno original de Debian, en el momento de apagar veremos que aparece un aviso mencionando que el software se está encargando de eliminar esta dichosa memoria.

Para mayor seguridad en la eliminación de RAM, ver el capítulo “secure delete M(sdmem)”. En el ca-

so de que el USB donde guardamos el texto estuviera cifrado con Truecrypt (TC) deberéis llevar otro USB con el programa dentro de él para extraerlo y descifrar el USB del archivo (también podríais descargarlo directamente de su web y extraerlo ahí mismo, pero mejor estar poco rato en el locutorio). Para más información sobre este uso de TC debéis mirar en el capítulo de Truecrypt: sección "cifrar USB".

Además de este uso que acabamos de mostrar y del que podemos estar bastante relajadas en cuanto a un poco de seguridad y anonimato, Tails también tiene otras aplicaciones, como la herramienta de *contraseñas y claves de cifrado*, que podréis usar para gestionar y configurar vuestras claves OpenPGP. Para sobreescribir archivos y dificultar su recuperación se puede usar Wipe, que en el momento de clicar con el botón derecho sobre un archivo aparecerá una opción que dice *Wipe* y que servirá para eliminar los datos. Si la seleccionamos deberemos clicar en la nueva ventana

***Options – 38* y marcar la casilla *Last pass with zeros instead of random data*.**

PROXYCHAINS

Proxychains es un programa disponible solamente para GNU/Linux y Unix que nos permite crear cadenas de proxies, “ocultando” así nuestra IP pública real en todo tipo de conexiones (HTTP, FTP, SSH, etc…). Esto se traduce en que podemos navegar por Internet o realizar cualquier operación en la red de redes sin descubrir nuestra identidad real.

¿Cómo funciona esto? ¿Es realmente posible?
¿Podría ocultar mis pasos en Internet?

Para poder conocer la respuesta a estas preguntas es necesario tener una mínima noción de lo que es un proxy en la jerga informática.

¿Qué es un proxy?

Un proxy puede definirse como un ordenador o servidor en el cual está corriendo un servicio de proxy, es decir, un “programa” que permite a ese ordenador actuar de intermediario entre nuestro ordenador y el destino final. En este caso, Proxychains nos ofrece conectarnos a más de uno en cadena.

Lo que significa que cuando navegamos por la red

podemos usar estos “ordenadores” y utilizarlos incluso en cadena, para dificultar el rastreo de nuestras búsquedas. De esta manera si usáramos un proxy de México y otro de la India. Si rastrearan la búsqueda tardarían en encontrarnos, sobretodo si el proxy que usamos es anónimo, que incluso podría no dar información de quien se habría conectado a él. Lo malo que tiene este sistema es que es tremendamente lento y si no tienes una conexión de esas potentes, no vale la pena.

Instalando Proxychains

Para instalar Proxychains sólo debemos abrir la terminal de Linux y escribir: sudo apt-get install proxychains

Configurando Proxychains.

Crear una cadena de proxies con Proxychains es muy sencillo. Solo necesitaremos el programa instalado, un editor de texto plano y conexión a Internet para buscar nuestros proxies (por supuesto, si ya tienen vuestros propios proxies no la ne-

cesitarán). Una buena lista de proxies es esta:

http://www.proxies.by/proxy/?rule1

(Recomiendo tener varias páginas desde donde descargar los proxys ya que a veces no se encuentra lo que se quiere y sobretodo, nunca a la primera)

Busquemos donde los busquemos siempre tenemos que tener en cuenta que soporten el protocolo HTTPs, ya que si queremos usar los proxies para navegar por Internet lo necesitamos, o por el contrario, no podremos hacerlo.

Una vez tengamos nuestros servidores elegidos, procedemos a editar el archivo de configuración:

sudo gedit /etc/proxychains.conf

Si no lo hemos modificado anteriormente, este archivo debería constar de un pequeño manual de como configurarlo.

La mejor opción es deshabilitar "dynamic_chain", es decir borrar el # antes de la línea. Ahora, y preferentemente al final del archivo para facilitar su lectura, añadiremos las direcciones de los proxies

con el siguiente formato:

socks5 77.91.195.16 3128

socks5 188.93.20.179 8080

socks5 216.155.139.115 3128

Donde socks5 es el tipo de proxy, seguido de la dirección IP y del puerto a usar. En vez de socks5, también podemos usar socks4 y http (los proxys https no se indican con "https" si no con "http").

Una vez añadidos, guardamos los cambios y cerramos el editor.

A continuación para usar el programa, sólo tenemos que teclear en la terminal: proxychains nmap, o proxychains firefox o la aplicación que sea...

Otra manera de usar proxychains

Para usar proxychains también podemos hacerlo instalando directamente proxychains + tor, de esta manera en terminal quedaría algo así:

sudo apt-get install proxychains tor

De esta manera estaremos instalando Proxychains, además de Tor (si bien no instalamos to-

do el programa de tor, para instalar tor es como se ha informado antes y aun teniendo instalado tor en nuestro Linux hay que pensar que “tor browser” es como un portable), y estará utilizando el proxy de Tor.

Para ejecutar de esta forma el programa deberemos abrir el terminal y la sintaxis será la misma: proxychains firefox .

Sólo que de esta forma no deberemos cambiar el archivo que antes requería modificarse.

VPN
(VIRTUAL PRIVATE NETWORK)

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, encriptación o la combinación de ambos métodos.

Desde mi punto de vista, una VPN es el mejor método para el anonimato en la red. Mi conclusión reside en el hecho de que "Anonymous" aconseja utilizarlo para el "hacktivismo".

Además de que con VPN la velocidad de red es la misma o casi la misma que sin VPN, mientras que en otros métodos como Tor o utilizando proxys la velocidad se ve tremendamente afectada.

Hay dos maneras de utilizar VPN, depende del distribuidor hay de pago o gratuitas. Es cierto que Anonymous desaconseja utilizar VPN gratuitas para hackear, pero debemos tener en cuenta el uso que le quiera dar cada una.

Cuando pienses en ponerte un servicio de VPN, primero plantéate la legislación del país. Una VPN estadounidense puede entregar tus datos fácilmente ante la emisión de una orden judicial. En otros países, como Suecia o Islandia, sería improbable, pues tienen una fuerte política de privacidad, lo cual hace que sea más difícil para las agencias de la ley acceder a ellos. Además, algunos servidores no guardan logs (registros) de los usuarios. También intenta conseguir servicios de una VPN que acepte pago anónimo (para aquellos que guardan datos sobre la facturación). Lo que hace la VPN es ocultar tu IP, y tú puedes escoger entre diversas IP correspondientes a distintos países. Cuando elijas un servicio

VPN asegúrate de que no sea de tu país sino de uno donde al rastrear tu IP sea difícil encontrar tu información privada como decíamos.

A continuación os dejo una lista que he extraído de la web de “hispanon”. Hay gratuitas y de pago. De todos modos puede que algunas estén desactualizadas o ya no existan.

También dejaré las que seguro existen y que personalmente las he probado tanto en Windows como en Linux.

Servicios Comerciales VPN [Recomendadas]:

http://www.swissvpn.net

http://www.perfectprivacy.com

https://www.ipredator.se

http://www.anonine.se

https://www.vpntunnel.se

VPN gratuitas (No recomendables):

http://cyberghostvpn.com

http://hotsposshield.com

http://proxpn.com

https://anonymityonline.org

Personalmente he utilizado para Windows "cyberghostvpn" y no tengo ninguna queja.

Para Linux no hay tantas opciones como para Windows o incluso Android o Mac (para las que también están disponibles), pero el caso es buscar y quien busca encuentra.

Hay varias opciones como por ejemplo "torvpn",

pero el servicio gratuito está muy limitado en cuanto al tiempo de uso y la configuración para neófitas en Linux es bastante complicada. En cambio "Securitykiss" es muy fácil de configurar y el resultado es muy complaciente. Existe "vpnbook" pero no la he probado y personalmente no puedo decir nada de ella.

Así pues, podemos utilizar para:

Windows:

http://www.cyberghostvpn.com

http://www.hotspotshield.com

Linux

http://www.vpnbook.com

https://www.securitykiss.com

http://www.torvpn.com

No vamos a detallar como instalar una VPN, ya que eso depende de cada red que se quiera descargar e instalar. De todos modos, como siempre, en Windows y sobretodo para quien no esté muy acostumbrada a Linux, instalar las VPN es muy fácil. En Linux la cosa se complica un poco, depende de

cual escojamos. Si queremos instalar Torvpn, la instalación es bastante complicada, mientras que por el contrario, la instalación de SecurityKiss es muy sencilla y no conlleva demasiados dolores de cabeza.

Aun así, como siempre se recomienda encarecidamente...

¡USAD LINUX!

PROXY WEB

Este apartado desde mi punto de vista no lo tengo muy claro ya que no lo he utilizado demasiado, pero no por ello voy a dejar de mostrarlo. Estas web se basan en que vosotras, a la hora de querer buscar información en la red de una manera “anónima”, utilicéis el proxy que os ofrece la web. Así estaréis navegando de manera “segura”. Para encontrar páginas de este tipo, con que busquéis en ixquick “proxy web” o algo así, encontrareis las que queráis. De todos modos dejo a continuación un para que sepáis un poco como uncionan.

http://proxyweb.com.es

http://proxyanonimo.es

Como mencionamos arriba es algo que no se ha experimentado demasiado ya que es fiarse de la buena fe de estos sitios, y por desgracia es algo que no sobra demasiado en los tiempos modernos. Así que es preferible que cada una controle lo que hace y sea una misma responsable de sus propias acciones.


HIDE IP MEGAPACK

Otro modo de navegar "anónimamente" es encontrar algún software que oculte nuestra IP. Este tipo de programas son parecidos a Tor, teniendo en cuenta que lo que deseamos con estos, es que nuestro rastro a la hora de hacer búsquedas quede camuflado.

Para encontrar alguno que nos haga navegar de manera anónima no hace falta buscar mucho, por lo menos para Windows ya que para Linux la cosa se complica, ya que escribiendo en la barra del buscador algo como *descargar navegar anónimo* salen muchos enlaces para descargarnos alguno. Cada programa de estos funcionan de una manera distinta, aunque la mayoría de ellos funcionan a base de proxys, así que con esta información sabemos que su velocidad queda diezmada a la hora de encadenar los proxys, si es que los encadenan.

En este caso voy a hablar de "Hide IP Mega Pack" y os voy a dejar el enlace para su descarga, ya que es realmente cómodo, bastante rápido, y algo debe tener, que hasta hace un par de meses que cerraron una web destinada a la información del activismo informático, había un paquete de aplicaciones para hacer "ataques DDOS" y entre estos, "Hide Ip" era el que mostraban como programa

para ocultar la IP y realizar el ataque.

Link del programa y el vídeo donde se enlaza a su descarga:

http://www.mediafire.com/download/1tral8tbb1twn69/Hide+IP+Mega+Pack+Por+TheChibaldo.rar

https://www.youtube.com/watch?v=ZUfG2qFdy0E

La instalación y uso de este programa es muy fácil, además de que en el vídeo ya explican como de instala.

"CIFRADO"

KLEOPATRA

Kleopatra es un software de código abierto destinado a encriptar archivos y correo electrónico.

En el capítulo donde se explica detalladamente como cifrar mensajes para una comunicación privada y segura, hemos visto que lo único que hacíamos con Kleopatra era descargarlo, instalarlo y listo. En ningún momento lo hemos usado y puede que a algunas les haya pasado por la cabeza que quizás no era necesario. Digo esto porque a mí me pasó.

El motivo de que no lo usáramos es que aunque no haga falta abrirlo, en realidad es él quien gestiona el cifrado de los mensajes. Del mismo modo que cuando estamos en Thunderbird y abrimos el administrador de llaves vemos las claves públicas y privadas que tenemos guardadas, si abrimos Kleopatra vemos que también las tenemos ahí, además de que podemos crear nuevas llaves públicas y privadas, importar nuevas claves o buscar certificados en los servidores de llaves.

En este caso vemos que es muy similar a Enigmail en cuanto a herramientas y utilidades. Debemos pensar que aunque no tuviéramos Enigmail podríamos enviar mensajes cifrados.

Bastaría con abrir un archivo de texto como LibreOffice Writer, cifrarlo y mandarlo como adjunto en un correo

normal sin cifrar.

Básicamente es lo que vamos a mostrar en este capítulo.

Debo reconocer que mis conocimientos sobre informática y más detalladamente en estos temas son muy limitados. Es por este motivo que para mandar un archivo adjunto cifrado, lo que hacemos con Thunderbird, al no haber indagado acerca del cifrado tipo S/MIME, utilizo Kleopatra para poder hacerlo. Seguro que hay otras formas, pero os mostraré la que conozco y que es bastante fácil.

No vamos a explicar cómo se instala ya que lo hemos visto en el capítulo de Thunderbird, pero sí vamos a ver cómo enviar esos adjuntos. Lo único que debemos tener en cuenta es que para cifrar un archivo y mandarlo debemos encriptarlo con la llave pública de nuestro destinatario de igual modo que si se tratara de un mensaje... Ya que cómo hemos visto antes la comunicación cifrada se basa en: Se cifra con la llave pública del destinatario y se descifra con la privada de quien recibe el mensaje.

Para cifrar un archivo, seleccionamos este en el directorio donde se encuentre, pulsamos encima con el botón derecho y seleccionamos *acciones – cifrar archivo*. E-

mergerá una ventana con varias opciones, entre ellas si queremos comprimirlo (esto nos permitirá poder mandar un directorio y no tener que comprimirlo antes), cifrarlo, firmarlo y si queremos eliminar el archivo original después de cifrar.

Esta opción depende de lo que queramos, ya que si queremos mantener el original después de mandarlo, debemos tener en cuenta que desde el momento que lo ciframos con la llave de otra persona nunca más podremos abrirlo ya que no dispondremos de su llave privada para descifrarlo.

Clicaremos en *Siguiente* y escogeremos el certificado (llave) con el que encriptar el archivo. Marcaremos *Cifrar* y ya lo tendremos cifrado y listo para mandar.

Veremos que la extensión del archivo es .gpg, mientras que las extensiones de las llaves son pub.asc si es pública, o pub.sec.asc si es el par de llaves pública y secreta.

Con Kleopatra también podemos de esta forma, cifrar archivos dentro de nuestro PC y tenerlos guardados con la confianza de que nadie los pueda ver, siempre y cuando la contraseña sea buena (aunque a estas alturas ya lo serán, no?)

Una pequeña desventaja que tiene Kleopatra, es que E-

nigmail permite crear los pares de llaves con mayor cantidad de bits.

En Enigmail llega a 4096 bits, mientras que Kleopatra alcanza 3072.

En Linux también existe Kgpg, normalmente viene incluso por defecto en algunas distribuciones y se encuentra en los repositorios. Lo podemos descargar del Centro de Software y tiene las mismas utilidades que Kleopatra. Como siempre utilizo Kleopatra no me he parado mucho con Kgpg, pero supongo que si no son idénticos, casi lo serán.

AESCRYPT

Aescrypt es un programa que se encuentra disponible para Windows y Linux, y que encripta archivos y carpetas con el sistema avanzado Advanced Encryption Standard “AES”. Por lo visto, algunos de los archivos que Wikileaks filtró y que le supusieron el cierre junto con todo el circo mediático que acompañó a las historias que destapó, fueron cifrados con este programa. Si no con este, de todos modos se podrían descifrar bien con Aescrypt.

La descarga, instalación y desarrollo del programa son distintos como suele suceder, en Windows o en Linux.

Para descargarlo deberéis acceder a http://www.aescrypt.com/download/ y allí encontraréis las distribuciones para los dos sistemas que usamos en esta guía.

Para instalarlo en Windows seguiréis los pasos habituales y una vez instalado, para encriptar el archivo deseado, solo hay que hacer clic con el botón derecho encima del archivo, seleccionar *AES Encrypt*, y aparecerá una ventana que pedirá la contraseña.

Esta será la que vosotras queráis. A partir de ahí el programa se encargará de cifrarlo con este sistema. Para descifrarlo haréis lo mismo, con la diferencia que haréis clic en *AES Decrypt*, de nuevo la contraseña y listo.

En la versión de Linux hay que descargar el "install.gz". Una vez descargado iréis a la carpeta donde se habrá alojado y lo descomprimiréis, le daréis permisos de ejecución y después lo instalaréis. Para hacer esto deberéis hacer unas cosas en el terminal y otras en modo gráfico.

Una vez estáis en la carpeta que tiene el programa. Hacéis clic derecho encima del archivo comprimido y seleccionáis *Extraer – Extraer aquí, autodetectar subcarpeta*. Aparecerá un solo archivo que termina con la sintaxis "install". Ahora abriremos el terminal y nos dirigiremos a la carpeta donde está, por ejemplo Descargas.

cd Descargas && ls (con "ls" aparecerán todos los archivos que estén dentro de *Descargas*)

chmod +x AESCrypt-GUI-1.0-Linux-x86-Install

sudo ./AESCrypt-GUI-1.0-Linux-x86-Install

Con esta última línea procederemos a instalar el programa en nuestro Linux. A partir de aquí se abrirá una ventana que os preguntará el idioma y esas cosas típicas como si fuera un programa de Windows.

Una vez lo tengamos instalado, para encriptar archivos

deberemos hacerlo desde la línea de comandos, o desde el modo gráfico. Primero lo explicamos desde el terminal y luego pasaremos a hacerlo en su alternativa gráfica.

Si abrimos un terminal y escribimos aescrypt, nos aparecerá en modo de ayuda, la sintaxis que se debe utilizar para cifrar o descifrar archivos.

Esta es:

usage: aescrypt {-e|-d} [{ -p <password> | -k <keyfile> }] { [-o <output filename>] <file> | <file> [<file> ...] }

Como veis es un lío, así que mostraremos una manera un poco más sencilla. Pongamos que el archivo que se quiere cifrar está en la carpeta /home/Manual/Escritorio/cifrados, y el archivo se llama acab.doc (ya nos dice que mejor no esté muy a la vista, no?), y la contraseña bastardxs (muy original).

La sintaxis para encriptarlo sería:

cd /Escritorio/cifrados && ls aescrypt -e -p bastardxs acab.doc

Una vez cifrado el resultado sería un archivo al lado del anterior que se denominaría acab.doc.aes. Como habréis observado el funcionamiento de esta herramienta es de lo más fácil y no requiere demasiadas complicaciones.

Hay que tener en cuenta un dato muy importante, y es que con AesCrypt NO podremos cifrar carpetas, así que si queremos cifrar varios archivos de una sola vez, deberemos comprimirlos antes para posteriormente cifrarlos. Podremos comprimir en .zip, .rar, o lo que os dé la gana

NOTA: Pensad que el archivo original no desaparece. Cuando hemos visto la opción de cifrar con Kleopatra donde el resultado sería acab.doc.gpg, nos pregunta si queremos eliminar el archivo original después de cifrarlo. Con Aescrypt no ocurre esto. Si queréis eliminar definitivamente el archivo original deberéis hacerlo con alguna de las herramientas que se encuentran al final de la guía y que se encargan de eliminar completamente los archivos.

Para descifrar el archivo la sintaxis sería:

```
aescrypt -d -p bastardxs acab.doc.aes
```

Para cifrar y descifrar desde el modo gráfico, lo que se debe hacer es ir hacia el archivo en cuestión, hacer clic derecho encima de éste y seleccionar *Abrir con – Otros*. Aparecerá una ventana con la que navegaremos hasta *Utilidades – Aescrypt* y aceptaremos. Una nueva ventana nos pedirá un par de veces la contraseña que queremos dar y automáticamente aparecerá el archivo cifrado. Para descifrarlo haremos lo mismo, pero el resultado es el archivo descifrado.

Es un programa muy útil, sobretodo si creamos una contraseña fuerte que impida que se pueda descubrir con un ataque de fuerza bruta. Por lo que estamos comprobando, el protocolo de cifrado AES es realmente bueno, pero hay herramientas muy potentes capaces de hackear contraseñas y acceder a la información deseada por quien dirija el ataque, así que hay que pensar bien qué es lo que hacemos.

Para las que tengáis dudas sobre qué programa utilizar para cifrar archivos, entre este o Kleopatra, mi consejo es que utilicéis éste para cifrar archivos personales y que uséis Kleopatra para cifrar archivos que a posteriori se mandarán por correo. Pienso que es mejor así ya que en el caso contrario hay que mandar la contraseña del archivo a la destinataria, con lo que siempre es un fallo

de seguridad, y de esta manera enviando un cifrado con Kleopatra lo mandaremos con la llave de la destinataria y ni siquiera nosotras tendremos la contraseña.



CCRYPT

Ccrypt es un programa que está disponible para un montón de distribuciones, entre ellas Linux y también en Windows 95, 98, 2000 y NT. La verdad es que sólo lo he usado en Linux y no creo que esté disponible para Windows 7 o estas últimas distribuciones de Microsoft.

Es un programa que hace lo mismo que el anterior, cifra con el mismo sistema AES y funciona de la misma manera, con algunas pequeñas diferencias.

Vamos a hacer la explicación de su instalación y funcionamiento en Linux que es para lo que creo que lo podréis usar. Para instalarlo bastará con abrir el terminal y escribir:

sudo apt-get install ccrypt

Para ejecutarlo bastará con escribir:

ccrypt -e archivo_en_cuestión

Nos preguntará la contraseña de seguridad un par de veces y aparecerá el archivo cifrado en la carpeta correspondiente.

Para descifrarlo:

ccrypt -d archivo_en_cuestión.cpt

NOTA: Podréis observar que una de las diferencias con Aescrypt es que aquí la terminación es ".cpt", además

de que ahora el archivo original ha desaparecido. Una vez lo descifréis volverá todo igual que estaba al principio.

Para cifrar o descifrar una carpeta:

ccrypt -eR nombre_de_la_carpeta

ccrypt -dR nombre_de_la_carpeta

Tened en cuenta que la carpeta no se cifra. Lo que hace es cifrar su contenido. Por estos motivos personalmente prefiero

Aescrypt a la hora de trabajar con archivos cifrados, pero cómo para gustos, colores. He querido dejar la información sobre este programa.

TRUECRYPT

¿Qué características podemos encontrar en Truecrypt?

-Puede crear un disco virtual cifrado dentro de un archivo, montándolo como si se tratase de un disco real.

-Permite cifrar una partición completa e incluso todo un dispositivo de almacenamiento, como un disco duro o una memoria USB. Puede cifrar una unidad, o una partición, donde esté instalado Windows.

-El cifrado se produce de forma automática, en tiempo real y de forma transparente.

-Ofrece diferentes niveles de denegación, en caso de vernos obligados a revelar la contraseña: Volúmenes ocultos (se tiene un volumen TrueCrypt dentro de otro volumen TrueCrypt). O sistema operativo oculto.

-Los volúmenes de TrueCrypt no pueden ser identificados, ya que no se diferencian de los datos aleatorios.

-Soporta diferentes algoritmos de cifrado como AES, Blowfish, CAST5, Serpent, Triple DES, y Twofish o una combinación de los mismos.

Estas son las principales funciones de Truecrypt y si os habéis dado cuentan básicamente lo que hace Truecrypt es encriptar, por resumir un poco e ir al gra-

no. Encripta volúmenes (directorios), encripta usb, los usuarios de Windows tienen la posibilidad de cifrar el sistema entero, y una de las mejores características es que encripta volúmenes ocultos.

Vamos a entrar a detallar un poco más cada una o varias de estas opciones, su descarga e instalación, tanto para Windows como para Linux, pero antes vamos a comentar esto de los volúmenes ocultos.

Como veremos más adelante, un volumen cifrado por Truecrypt, no es más que una carpeta cifrada con un algoritmo que usa para que nadie, excepto quien tenga la contraseña, vea lo que hay en su interior. En esta carpeta guardamos todo lo que queramos o nos quepa, depende del tamaño que le hayamos asignado. Pues bien, dentro de esta,carpeta podemos crear otra carpeta de la que según parece, y digo esto porque al no ser informática (y siendo algo pragmática) no puedo asegurar nada que no haya podido demostrar yo misma, no hay ningún rastro. Lo único que podremos comprobar es que si observamos la capacidad de almacenamiento de la carpeta, los MB usados y los MB restantes, vemos que no hay ninguna prueba evidente de que dentro de ella, haya otra carpeta oculta con su tamaño correspondiente.

Por ejemplo, si el volumen es de 100 MB y el oculto es de 50 MB, en principio debería verse esos 50 MB por a-hí que faltan, pero nada, no hay rastro. Además, aun-que algún hacker policial pudiera intuir que está esa carpeta, Truecrypt no guarda ningún registro (y eso sí he leído que hay gente que ha buscado algún registro como locos y nunca lo han encontrado), con lo que tam-poco podrían creer durante mucho tiempo que sí existe ese volumen. En este caso todo serían suposiciones.

Hay ciertas diferencias desde la versión de Windows a la de Linux, hay algunos cambios que no suelen haber en los programas y que no imaginas que pudieran estar en este. Es cierto que Linux tiene un nivel muchísimo mayor que Windows en cuanto a seguridad y cifrado, ya que puedes cifrar desde el momento de la instalación del sistema operativo todo el contenido o particiones. Pero aun así se agradecería que Truecrypt pudiera cifrar la distribución entera, aunque imagino que si no lo hace es porque no se debe poder.

El último comentario que hago por ahora, que también es una desventaja para las usuarias de Linux, es que no intentéis buscar el paquete de idioma español ya que, mientas que lxs que utilicen Windows bastará con de-scargar el paquete correspondiente y guardarlo en el di-

rectorio de la ubicación del programa para poder cambiar a éste, las que usen Linux no podrán. Es una manera de que aprendamos inglés, o sea, es una ventaja más de Linux. O no?

Descarga e instalación

Para descargar Truecrypt, tanto si es para Windows o Linux deberéis ir al siguiente enlace:

http://www.truecrypt.org/downloads

Aquí simplemente deberéis escoger vuestra distribución y descargarla.

Para instalar Truecrypt en Windows bastará con clicar un par de veces en el paquete descargado y seguir la instalación como siempre se hace con cualquier paquete.

La instalación de Linux es algo distinta. Por un lado podéis descargar el código fuente y compilarlo vosotras mismas, pero es algo para usuarias experimentadas.

Para las que hayáis escogido el paquete “standard-32bits” habréis descargado un archivo .tar.gz. Para instalar deberéis ir a la carpeta de descargas o donde lo hayáis guardado y clicar con el botón derecho y seleccionar *extraer aquí, autodetectar subcarpeta*.

Una vez esté descomprimido, clicáis sobre el archivo que aparezca con el botón derecho de nuevo y esta vez teclearéis *propiedades – permisos,* habilitaréis la pestaña *es ejecutable* y después *aceptar*. Una vez hecho esto pulsad encima del archivo y aparecerá una ventana del terminal que os pedirá si queréis instalar el programa o extraer el archivo. Pulsad el 1 y os mostrará los términos y condiciones del servicio. Cuando os aparezcan, con la tecla de la flecha dirigida hacia abajo del teclado descenderéis hasta que os aparezca la frase de aceptar los términos. Una vez aceptados se habrá acabado la instalación y Listo!

Truecrypt instalado.

Es posible que por el motivo que sea no podáis usar esta manera de instalarlo, o que prefiráis utilizar la terminal para hacerlo. En este caso abrís el terminal:

cd Descargass (o donde esté descargado) tar xzf truecrypt-7.1a-linux-x86.tar.gz (o la distribución descargada) chmod +x truecrypt-7.1a-setup-x86 ./truecrypt-7.1a-setup-x86

Una vez que el programa está instalado, las usuarias de

Windows tenéis la posibilidad de cambiar Truecrypt al idioma que queráis. Para pasar el programa a español, basta con descargar de este enlace:

http://www.truecrypt.org/localizations el paquete que necesitéis, lo descomprimís en el directorio donde se ubica el programa *Archivos de programa – TrueCrypt* y una vez hecho ste paso, ejecutaréis el programa y es posible que ya haya cambiado el idioma. En el caso contrario clicaréis en *Settings – Language* y seleccionáis el que queráis.

Antes de meternos en faena quiero aclarar que las explicaciones sobre el uso de truecrypt las he extraído de la red, más explícitamente de una página que encontraréis al final del manual. He decidido hacerlo así y no explicarlo yo misma, ya que excepto algunas aclaraciones que irán saliendo, está explicado de manera muy sencilla.

Otro motivo por el que se ha decidido hacer, casi, un corta y pega, es que dada la importancia de este programa no quiero obviar ni olvidar nada que pudiera pasarme por alto.

De todos modos recomiendo utilizar otras fuentes, disponibles en el libro, ya que en ellas hay imágenes, lo que seguro hará más agradable la instalación y aplica-

ción del programa

Crear un volumen cifrado

De momento vamos a ver cómo crear un volumen o archivo contenedor cifrado, pero sencillo. Más adelante veremos cómo crear uno oculto para mayor seguridad de nuestros datos.

Después de instalar el programa tendréis Truecrypt en alguna parte del ordenador. Seguramente en Windows lo tendréis en el mismo escritorio y el Linux lo tendréis en *Aplicaciones – Utilidades*.

Una vez localizado deberemos ejecutarlo y aparecerá la ventana principal del programa.

Para crear un nuevo contenedor, debes hacer clic sobre el botón *Create Volume*. Verás que aparece una nueva ventana con un asistente que te guiará a lo largo de todo el proceso.

Para empezar, debes asegurarte de que tienes seleccionada la primera opción: *Create an encrypted file container*. A continuación, sólo tienes que hacer clic en el botón *Next*.

Lo siguiente que debes decidir es si tu contenedor será

estándar u oculto. De momento, creo que debemos conformarnos con el primero. Por lo tanto, te aseguras de que está seleccionado *Standard TrueCrypt volume* (que es el valor por defecto) y haces clic en el botón *Next*.

En el siguiente paso, debes decidir dónde ubicas tu archivo contenedor. Puedes optar por escribir directamente en el cuadro de texto, incluyendo la ruta completa y el nombre del archivo, o puedes hacer clic en el botón *Select File* … para obtener una ventana que te simplifique la elección de la ruta.

Si has hecho clic en el botón, te aparece una ventana, donde puedes escribir el nombre del archivo y elegir el lugar donde se creará, en la lista desplegable o eligiendo *Buscar otras carpetas.*

En cualquier caso, el resultado será el cuadro de texto de la ventana anterior debidamente relleno. Sólo quedará hacer clic de nuevo en el botón *Next*.

Se supone que el siguiente paso es el más importante, ya que en él puedes elegir el método que se aplicará para cifrar la información dentro del archivo contenedor. Sin embargo, para usos normales, pienso que cualquiera de ellos es más que suficiente. Cuando te hayas decidido por uno (o por una combinación de ellos), sólo

tienes que hacer clic en *Next* para seguir.

****** Según algunas fuentes cómo por ejemplo, http://foro.elhacker.net/criptografia/cual_es_el_mejor_algoritmo_de_encriptacion_de_truecrypt-t358949.0.html, el mejor algoritmo de cifrado de truecryt es “AES-Twofish-Serpent” ******

El siguiente paso consiste en establecer el tamaño del contenedor. Basta con escribir el número y elegir en la lista la unidad de medida. Como puedes leer en la misma ventana, hay que tener en cuenta que el tamaño mínimo de una unidad FAT es de 275 KB y el de una partición NTFS es de 2829 KB.

Una vez establecido, debes hacer clic de nuevo en el botón *Next*.

A continuación deberás escribir tu contraseña. Recuerda que este es el paso más delicado y que, según tu elección, tus datos serán más o menos vulnerables. En esta ventana se pueden leer, además, las recomendaciones típicas para elegir una buena contraseña (utilizar varias palabras, mezclar caracteres no alfanuméricos, etc)

La contraseña debe escribirse dos veces por precaución

(para prevenir posibles errores tipográficos). Cuando termines, haz clic en el botón *Next*.

El siguiente paso consiste en elegir el sistema de archivos con el que se formateará el contenedor. Si vas a utilizarlo en diferentes sistemas operativos, una forma de asegurar la compatibilidad es elegir FAT. Una vez elegido el sistema de archivos, debes hacer de nuevo clic sobre el botón *Next* para continuar.

En la siguiente ventana se calculan los valores aleatorios que se utilizan como base para cifrar los datos. Para conseguirlo, se utilizan como referencia los movimientos del ratón.

Después de mover el ratón durante algo de tiempo y de la forma más aleatoria posible, puedes hacer clic sobre el botón *Format*.

Cuando acabe, aparecerá una ventana informando de la situación. Aquí sólo hay que hacer clic en *Aceptar.*

Por último, obtenemos un mensaje que nos indica que el volumen se ha creado satisfactoriamente y que está listo para usarlo. Si queremos repetir el proceso y crear un nuevo contenedor, podemos hacer clic en el botón *Next*. Si no es así, pulsaremos el botón *Exit.*

Antes de ver cómo utilizar el volumen, hay que aclarar

que la opción de crear el volumen cifrado es casi idéntica en Linux o en Windows, así que no hace falta hacer otro manual con la creación del volumen en Windows. Realmente se va a usar un ejemplo en cuestión, ya sea de Windows o Linux para demostrar cómo funciona el programa. Dadas las similitudes entre la manera de hacerlo con un sistema u otro, sería demasiado largo y redundante hacerlo de las dos maneras.

TRUECRYPT II

Utilizar el volumen

Para utilizar el contenedor que hemos creado en el punto anterior, sólo hay que ejecutar TrueCrypt y, en la ventana inicial del programa, hacer clic en el botón *Select File.* Si conoces la ubicación de tu archivo contenedor, puedes escribirla en el cuadro de texto que hay junto al botón.

Utiliza la ventana que aparece para buscar tu archivo y, una vez localizado, selecciónalo y haz clic sobre el botón *Abrir*.

De vuelta en la ventana principal, sólo queda montar la nueva unidad. Tienes que seleccionar un Slot (por ejemplo el uno) y hacer clic en el botón *Mount*.

Lógicamente, antes de montar la nueva unidad, TrueCrypt debe pedirnos la contraseña que introdujimos al crear el contenedor. Una vez escrita, sólo tienes que hacer clic en el botón *Aceptar*.

Una característica que a mí me resulta un poco molesta es que, para montar una unidad, también necesita privilegios de administración (en Linux). Por ese motivo, TrueCrypt también solicita la contraseña de root.

Si las contraseñas son correctas, verás que el con-

tenedor aparece en el Slot 1.

Desmontar el volumen

Esto parece una tontería, pero hay que tener siempre muy presente que cuando se quiera cerrar el programa y que los datos vuelvan a estar bien cifrados, después de cerrar la ventana de "dolphin", "nautilus" o "windows", hay que pulsar siempre encima de *Dismount*. De esta forma los datos quedarán bien guardados y seguros. De lo contrario sería más fácil, aunque reiniciáramos el ordenador, acceder a la información ya que quedaría un registro hecho por el ordenador, aunque Truecrypt no lo hubiera hecho.

Cifrar una partición o un USB

A continuación vamos a ver cómo cifrar una partición (por ejemplo /home en Linux) o un pendrive. Antes de seguir hay que recordar que la partición que se vaya a cifrar se va a formatear con lo que deberéis hacer una copia de seguridad de los datos o guardarlos en otro lugar de momento.

Para comenzar, desde la ventana principal del programa, el primer paso consistirá en hacer clic sobre el botón *Create Volume.*

Verás que aparece una ventana donde puedes elegir entre *crear un archivo contenedor encriptado* o *crear un volumen dentro de un dispositivo o de una partición*. Esta segunda opción es la que nos interesa hoy, luego, hacemos clic sobre ella y continuación en el botón *Next*.

En el siguiente paso, el programa te ofrece la posibilidad de elegir entre un *volumen estándar* o un *volumen oculto*. De momento nos interesa la primera opción, quizás otro día dediquemos nuestra atención a la segunda. Por lo tanto, debes hacer clic sobre ella y, a continuación, de nuevo en *Next*.

Debes elegir el dispositivo que vas a cifrar. Puedes escribir el nombre del dispositivo en el cuadro de texto, pero, para evitar errores, te recomiendo que hagas clic en el botón *Select Device.*

Después aparece una ventana con todos los dispositivos de almacenamiento que tenemos conectados a nuestro ordenador. Debes tener cuidado, un error al elegir el dispositivo puede hacer que pierdas toda la información que contenga. Recuerda que el dispositivo elegido va a formatearse. No obstante, si te fijas en el directorio de montaje, es muy fácil identificar el dispositivo correcto. Al volver a la ventana del asistente, verás que ya está se-

leccionado el volumen adecuado. Como de costumbre, para seguir, sólo hay que hacer clic en el botón *Next.*

Bueno, creo que si has llegado hasta aquí, el mensaje que te muestra ahora Truecrypt está un poco de más. En él, encontramos una recomendación para usuarias inexpertas donde nos sugiere que, en lugar de cifrar un dispositivo completo, creemos un contenedor. Si optamos por esta segunda opción, podremos tratarlo como a cualquier otro archivo y el resto de archivos de nuestra unidad no correríanningún tipo de peligro. Si estás seguro de continuar, haz clic en *Sí*.

En el siguiente paso, Truecrypt nos recuerda que la unidad que hemos seleccionado se va a formatear y que este paso implica la pérdida de todos los datos que contenga actualmente. Desde luego, si perdemos algún archivo, no podremos culpar al programa. Si aún estás seguro de seguir adelante, debes hacer clic en el botón *Sí.*

Los siguientes pasos son idénticos a los vistos en el artículo anterior. Para empezar, debemos seleccionar el algoritmo de cifrado que vamos a utilizar. Las opciones son *AES, Blowfish, CAST5, Serpent, Triple DES, y Twofish*, además de algunas combina-

ciones entre ellos. Puedes hacer clic en *More information on*... para obtener más detalles sobre el algoritmo que elijas. Cuando hayas tomado una decisión, debes hacer clic en el botón *Next* para continuar.

A continuación, escribiremos la contraseña que usaremos más adelante para acceder a nuestra memoria USB. Debemos de escribirla dos veces para estar seguros de que no cometemos ningún error tipográfico al escribirla.

En el siguiente paso elegimos el tipo de sistema de archivos que utilizaremos en el formateo de nuestra unidad. Si piensas utilizar tu memoria USB sólo en sistemas Linux, puedes utilizar ext3, pero si también piensas acceder a ella desde sistemas Windows, es muy recomendable que utilices FAT. En cualquier caso, después de hacer tu elección, haz clic sobre *Next* para continuar.

En la siguiente ventana se calculan los valores aleatorios que se utilizan como base para cifrar los datos. Para conseguirlo, se utilizan como referencia los movimientos del ratón.

Después de moverlo durante algún tiempo y de una forma lo más aleatoria posible, puedes hacer clic sobre el botón *Format*

para seguir.

Ahora sí. El sistema ya está dispuesto para comenzar el formateo de la unidad. Ya no habrá más posibilidades de arrepentirse. Por eso, a riesgo de parecer pesado, Truecrypt vuelve a preguntarte si estás realmente seguro de perder cualquier cosa que tengas en el PenDrive. ¿Estás realmente seguro de que no tienes datos importantes en tu PenDrive que no hayas copiado en otro soporte? ¿Seguro?. Pues ya puedes hacer clic en el botón *Sí* para iniciar el proceso de formateo.

A continuación, verás una barra de progreso que te indica el avance del formateado.

Cuando llegue a su fin, Se muestra una ventana informando de que el proceso ha concluido. Sólo queda hacer clic en el botón *Aceptar* para empezar a disfrutar de nuestro PenDrive protegido a prueba de curiosos.

Esta manera de cifrar una partición o pendrive, está explicada sobre el sistema de Linux. La verdad es que en Windows por desgracia no lo he probado y no sé si será muy distinta, aunque imagino que no. En el caso de que las usuarias de Windows os encontréis con algo raro, seguid a vuestra intuición y trabajad con cautela, no perdáis informa-

ción importante.

Utilizar la partición o USB

Una vez que hemos cifrado la unidad, ya sólo podremos acceder a ella desde Truecrypt, después de escribir la contraseña adecuada. Así que para utilizarla abriremos el programa y en su ventana principal, hacer clic sobre el botón *Select Device*...

En la ventana que aparece, seleccionas la unidad cifrada y haces clic sobre el botón *Aceptar*. Observa que ahora no aparece directorio de montaje, porque aún no está montada. De vuelta en la ventana principal de TrueCrypt, debes hacer clic en uno de los Slot que tienes disponible, por ejemplo en el primero y después sobre el botón *Mount*. Y a partir de aquí funcionamos igual que si quisiéramos abrir un volumen cifrado normal.

Crear volumen oculto

En la creación del volumen oculto hay algunas diferencias entre Windows respecto de Linux. Mientras que en Windows existe la posibilidad de hacerlo de dos maneras, creando el volumen oculto directamente dentro de un volumen cifrado ya creado anteriormente, o crear el oculto y el normal a lavez, Linux solo te deja crear los dos volú-

menes a la vez, de manera que si tienes otras carpetas cifradas no puedes añadirles una oculta. Tiene sus inconvenientes, pero por algún motivo se hará así. La manera de hacerlo en Linux seleccionando la opción *Hidden TrueCrypt volume*, se basa en que primero crearemos el volumen normal y siguiendo los pasos crearemos más tarde el oculto.

Para esta explicación no vamos a detallar paso por paso como en los ejemplos anteriores ya que es exactamente lo mismo que antes sólo que añadiendo unos pasos más para crear el oculto. De manera que: Abrimos Truecrypt y seleccionamos *Crear Volumen*. En la siguiente seleccionaremos *Crear un contenedor cifrado –*

***Volumen oculto Truecrypt* y a partir de aquí en Windows nos preguntará si queremos hacerlo del modo directo o el modo normal (éste es el modo que usaremos para explicar y es el modo que utiliza la distribución de Linux).**

Una vez seleccionado la opción, pasaremos a crear el volumen exactamente igual que se ha detallado antes creando el contenedor normal.

Nota: Toma en cuenta el tipo de documentos, su cantidad y tamaño que necesitan ser almacenados. Deja cierto espacio para el Volumen Común. Si se-

leccionas el tamaño máximo disponible para el Volumen Oculto, no serás capaz de colocar ningún archivo nuevo en el volumen Común original.

Si tu Volumen Común es de 10 Megabytes(MB) de tamaño y

tú especificas un tamaño de Volumen Oculto de 5MB, tendrás

dos volúmenes (uno oculto y el otro común) de

aproximadamente 5MB cada uno.

Asegúrate que la información que almacenas en el Volumen Común no exceda los 5MB que has fijado. Ello debido a que el programa TrueCrypt no detecta, por sí mismo, en forma automática la existencia del Volumen Oculto, y podría accidentalmente sobre-escribirlo. Te arriesgas a perder todos los archivos almacenados en el volumen oculto si excedes el tamaño previamente establecido. Para evitar esta situación intentad ir sobradas de espacio para los dos volúmenes.

Haremos todos los pasos igual que antes y terminada la creación de éste seguiremos adelante para generar el oculto.

Los pasos para crear este último, son los mismos

que los anteriores. Cuando hayamos terminado el proceso de creación de los dos volúmenes accederemos a la ventana principal de Truecrypt.

Utilizar el volumen

Para utilizar cualquiera de los dos volúmenes hay que tener en cuenta que para un mismo archivo, carpeta o volumen (o

como queramos llamarlo), tendremos dos contraseñas, a cada

cual más potente y segura, pero esto siempre puede llevar a

confusiones u olvidos.

Para ingresar al directorio oculto seguiremos los pasos

normales para ingresar a cualquier volumen cifrado de

truecrypt y guardaremos en él lo que queramos.

La importancia de esta característica de Truecrypt es

sobretodo algo que debemos intentar que no se nos olvide,

sobretodo cuando tengamos los volúmenes ya lle-

nos de

archivos y datos. Y es que cuando queramos abrir el volumen

normal, en el momento que nos pide la contraseña deberemos

acceder a *Opciones* que aparece en la ventana. Esta se abrirá y

habilitaremos el cuadrado de *Proteger el volumen oculto cuando*

***se monta el otro*, y pondremos debajo la contraseña del oculto.**

De esta manera nos ahorraremos la situación que se comenta

un poco más arriba acerca de sobreescribir los datos del otro volumen.

Keyfiles (Archivos Llave)

Truecrypt, por si con lo anteriormente mencionado no hubiera suficiente seguridad, nos ofrece la posibilidad de crear "archivos llave" o usar cualquier archivo como llave para acceder a los volúmenes. Estos archivos llave nos serán de gran ayuda sobretodo para aquellos casos en los que la contraseña no sea lo suficiente fuerte, y darán una

mayor seguridad a nuestros contenedores cifrados.

Desde mi punto de vista lo realmente bueno de estos archivos llave, es que a la hora de crear un volumen podremos usar cualquier archivo (ya sea una película, una imagen o lo que nos dé la gana) para bloquear el acceso al volumen. Esto significa que en el momento de querer entrar en el contenedor deberéis poner la contraseña y el susodicho archivo.

Para crear un archivo llave. En la creación de un volumen, cuando estéis en la ventana en la que hay que decidir la contraseña, pulsaréis en la opción que dice *Keyfile* y una vez en la otra ventana clicaréis en *Generate Random Keyfile.*

Aparecerá otra ventana donde deberéis mover el ratón para dar mayor fuerza al algoritmo y a la seguridad del archivo.

Cuando estéis listas clicaréis en *Generate and save Key*, con lo que ahora deberéis decidir donde guardar el archivo y el nombre que queráis.

Desde mi punto de vista es mejor, ya que en principio no habrá ningún registro ni rastro de su nuevo uso, utilizar cualquier archivo que tengamos en el

ordenador para usarlo como archivo llave. Para ello, en la misma ventana de la contraseña, clicaréis en *Keyfiles* y en la siguiente ventana pulsaréis en *Add files*. En este momento decidiréis qué archivo escoger para usarlo de llave y después *Ok*.

Ahora ya habremos escogido o creado un archivo de llave y lo único que queda es saber que cuando queramos montar el volumen, en el momento que nos pida la contraseña, clicaréis en *Keyfiles* y bastará con seleccionarlo.

No he comentado en la explicación que para usar estas llaves deberemos habilitar la casilla de *Use Keyfiles* en el momento de decidir usarlas, ya que se sobreentiende. Si alguien tiene algún problema que compruebe antes si estaba habilitada la opción de usarlas.

Hasta aquí esta explicación de los archivos llave. Creo que como mayor seguridad puede ser muy útil ya que el archivo lo podemos guardar donde queramos. Eso sí, habrá que tener cuidado de no perder ese archivo ya que sino no podremos entrar a nuestro volumen. Deberemos pensar siempre en hacer copias de seguridad de este archivo

Hacer de TrueCrypt un programa Portable

Esta opción es de gran utilidad aunque la usemos en pocas ocasiones, si por ejemplo queremos ir a un locutorio y nos encontramos en él con un USB que hemos cifrado por completo con TrueCrypt en nuestra casa. Dado que la única manera de poder acceder a la información que contiene el pendrive sería descifrándolo con TrueCrypt, tendríamos la posibilidad de descargarlo en el mismo locutorio, instalarlo y usarlo, pero esto sería un poco engorroso, sobretodo porque estaríamos dejando rastros de nuestro paso por el local.

Cuando nos disponemos a instalar el programa, ya sea en Windows o en Linux, nos pregunta antes de efectuar la instalación, si queremos instalarlo o extraerlo. Esta es la característica de hacerlo portable.

En Linux, una vez extraído el programa, éste se guardará temporalmente en la carpeta *tmp* y para entrar en ella deberemos ser superusuarias. Esta carpeta contendrá dos subcarpetas y dentro de la que dice *bin* encontraremos el archivo ejecutable *Truecrypt*.

Otras funciones

Como se ha dicho ya, Truecrypt tiene más características, como la de cifrar el disco duro entero

(opción para Windows).

Particularmente esta función es realmente útil, pero depende de varias especificaciones que debe cumplir la usuaria, como que el ordenador no tenga arranque dual (tener dos sistemas operativos en un disco duro), u otras características que harían que esta guía sobre seguridad informática para la activista se convirtiera en un manual exhaustivo acerca de este software.

De todos modos mi consejo es que exploréis al máximo este programa y que, hasta que no se conozca nadie capaz de hackearlo, tenedlo presente en vuestra seguridad.


SEGURIDAD MÓVIL


CORREOS CIFRADOS

1. Lo primero que deberemos hacer antes de nada es descargar las aplicaciones que serán necesarias para mandar correos encriptados. Esto como veréis será muy parecido a lo que habíamos hecho con Thunderbird a la hora de tener comunicaciones seguras.

Las herramientas que necesitaremos son (mejor descargarlas todas primero y luego empezad con el manual): ASTROAdministrador de archivos, APG, K-9Mail.

2. Una vez estén descargadas las aplicaciones lo primero que debemos hacer, es guardar en el móvil las llaves PGP que usamos para cifrar los mensajes en el PC. Para ello las guardaremos dentro del programa APG. Esta aplicación puede generar llaves públicas y privadas como lo hace

OpenPGP, pero además de que esa herramienta está en fase BETA lo que la hace un poco inestable, mejor será utilizar las que ya hemos creado con OpenPGP. Aunque pudiéramos crearlas con APG sería mejor usar siempre OpenPGP ya que las creará más fuertes y con mayor algoritmo de cifrado.

Para guardarlas deberemos conectar el móvil al ordenador.

Una vez esté conectado, abriremos el programa Thunderbird y nos dirigiremos a *OpenPGP – Administración de claves*. Nos situaremos encima de las claves y una por una las vuestro Android. Para guardarlas ahí haremos clic con el botón derecho encima de vuestro par de claves (mejor empezar por las vuestras) y seleccionaremos en la ventana que emerge *Exportar claves a un fichero – Exportar claves secretas* y navegaremos hasta la carpeta APG. Una vez tengáis todas las llaves instaladas.

Una vez estén guardadas las llaves desconectaremos el teléfono de la máquina y pasaremos al punto 3.

3. Instalar las llaves. Para instalarlas en el móvil, deberemos seleccionar el programa APG. Cuando éste arranque aparecerá una ventana con cuatro opciones. No seleccionaremos ninguna de ellas, en cambio seleccionaremos *Menú – Administrar llaves privadas*. Se abrirá una pantalla que estará vacía. Volveremos a pulsar *Menú – Importar llaves*.

Apareceréis en una nueva ventana y seleccionaréis la carpeta (lo que mejor creáis), pero no lo hagáis con alguna aplicación

del móvil. Si las herramientas de los ordenadores, tal como hemos visto, pueden ser vulneradas ima-

ginad una herramienta del teléfono.

4. Crear y configurar cuentas en K-9 Mail. Cerraréis APG y ahora hay que abrir K-9 Mail. Cuando lo abráis el programa irá indicando como deberéis crear y configurar las cuentas que tengáis. Es muy fácil e intuitivo por lo que no mostraremos como se hace. A estas alturas del manual ya sabréis configurar bien las cuentas. El único consejo es que lo hagáis delante del ordenador con Thunderbird abierto y comprobad antes de terminar de crear las cuentas, que la configuración del servidor de entrada y de salida sean los mismos datos, para que no haya ningún problema.

5. Una vez las cuentas estén creadas podremos enviar mensajes cifrados. Aquí, del mismo modo que cuando enviamos un mensaje cifrado lo mejor es firmarlo con nuestra llave, podremos hacer lo mismo.
Cuando hacemos clic en *Menú – Redactar*, en la pantalla de redacción, debajo de la casilla reservada para escribir la destinataria hay dos opciones que deberemos seleccionar para firmar y cifrar los mensajes. Mejor hacerlo cuando hayamos terminado de redactar el mensaje ya que en cuanto lo hagamos se abrirán un par de ventanas de APG. Al marcar *Firmar* se abrirá una

ventana y seleccionaremos nuestra llave para firmar el mensaje. Cuando seleccionéis *Cifrar* deberéis seleccionar la llave pública de vuestra destinataria.

6. Enviar y recibir. Para enviar, una vez hayamos redactado el mensaje y seleccionado *Cifrar*, pulsaremos *Menú – Enviar*. A continuación, si habéis seleccionado *Firmar,* hay que introducir la contraseña de vuestra llave y el mensaje se enviará.

Para recibir un mensaje cifrado, en el momento de abrirlo, veremos que éste está cifrado y que hay una opción que dice *Descifrar*. Escribís la contraseña de la clave y podréis leer el mensaje que os habrán mandado.

NOTA: Hay ocasiones en que no sabréis porqué, pero K-9 Mail no manda los mensajes y aparecen algunos mensajes de error. Para solucionar esto basta, normalmente, con dirigirse al control de aplicaciones de Android y reiniciar la aplicación.

En alguna ocasión esto no funciona y la solución pasa por desinstalar y volver a instalar el programa, volviendo a crear las cuentas. Lo bueno de K-9 Mail, es que acepta cualquier cuenta. Si tenéis Riseup no habrá problema para trabajar con él.

ENCRIPTAR DIRECTORIO

Para encriptar carpetas en Android existen varias aplicaciones que hacen eso, pero en esta ocasión vamos a mostrar cómo hacerlo con Cryptonite. Esta es una aplicación que trabaja con TrueCrypt, así que nos da un poco de confianza. Está todavía en fase BETA, así que no es tan fiable cómo TrueCrypt.

Como hemos comentado, aun conociendo estas herramientas, mejor no guardar información delicada en el teléfono.

Cryptonite tiene tres opciones en cuanto lo abrimos*: Dropbox, Local y Expert*. En esta guía trabajaremos con la opción *Local*, ya que con ella crearemos una carpeta encriptada y podremos guardar información en ella.

Cuando seleccionemos *Local*, debajo de la opción aparecerán otras opciones. Seleccionaremos *Create Local Volume*, y confirmaremos. Ahora deberemos seleccionar el tipo de cifrado que queremos entre las opciones que nos muestra. Lo mejor será elegir *Paranoia* que basa su cifrado en el algoritmo AES 256 y será más seguro. En la ventana que aparecerá

pulsaremos sobre la carpeta con el símbolo "+" que tiene incrustado (así crearemos una carpeta nueva.

Le daremos el nombre que queramos, y después de navegar hasta ella haremos clic sobre *Use current folder*. Pondremos la contraseña que queramos para el directorio encriptado y ya

tendremos una carpeta cifrada.
Para descifrarla y así guardar o extraer información, deberemos abrir el programa y seleccionar *Local – Decrypt local folder*. Navegaremos hasta la carpeta que antes hemos creado y pulsaremos sobre *Select current folder*. Deberemos escribir la contraseña y lo tendremos a punto de guardar lo que queramos.

APLICACIONES VARIAS

A continuación veréis una lista de aplicaciones de seguridad que os servirán para poder trabajar con Android un poco más tranquilas. Entre estas encontraréis herramientas para navegar por la red, llamar por teléfono o cifrar partes del móvil. No vamos a mostrar detalladamente cómo utilizar cada una de estas herramientas, como hemos hecho con las distribuciones de Windows o Linux, ya que el tema principal de este manual es la seguridad en vuestros ordenadores. De todos modos, el uso de estas aplicaciones no es muy difícil y seguro que quienes se decidan por utilizarlas no tendrán demasiados problemas a la hora de trabajar con ellas.

1. Hotspot Shield VPN

Esta aplicación está destinada a navegar bajo una red VPN.

En otro capítulo hemos mostrado el funcionamiento de las VPN y su efectividad a la hora de navegar anónimamente. Es gratuita, aunque tiene opción de hacerla de pago.

2 Obscura Cam

Esta aplicación se encarga de reconocer y pixelar las caras en las fotografías que tengáis guardadas en el móvil. Es una cómoda y efectiva herramienta para aquellas que acuden a las manifestaciones para hacer fotografías.

3. RedPhone

RedPhone encripta el contenido de las conversaciones que tenéis cuando hagáis una

llamada. Por supuesto RedPhone, sólo será efectivo cuando las dos partes (quien llama y la receptora) tienen instalado el programa. Como idea es genial, si un programa puede encriptar las conversaciones telefónicas. Pero sinceramente no diría nada “raro” por teléfono aunque tuviera instalados cien programas como este.

4. Orbot

Este es un software de navegación anónima que pertenece al colectivo Tor. Así que es una de las pocas aplicaciones de las que nos podemos fiar. Por lo menos quienes están detrás de
Tor sabemos que trabajan por generar una cultura de seguridad en la red. Para navegar es necesaria la siguiente aplicación 5. Orweb V2

Aplicación para navegar anónimo junto con Orbot.

6. Encryption Manager Lite

Esta aplicación es similar a Cryptonite. Bajo contraseña creará directorios cifrados en vuestros teléfonos.

7. Droidwall

Cortafuegos que controla las conexiones entre el teléfono y la red. Con él podréis escoger qué aplicaciones se conectarán y cuales no.

8. Crypt Haze

Aplicación para mandar mensajes cifrados. Para utilizarla deberéis tenerla, tanto quien envía el mensaje cómo la destinataria.

9. KeePassDroid

KeePassDroid es una herramienta de fácil uso

para la administración segura de contraseñas para tu dispositivo
Android.
10. Gibberbot
Gibberbot permite organizar y administrar tus diferentes cuentas de mensajería instantánea (IM siglas en inglés) usando una única interface. Utiliza software OTR para las comunicaciones autenticadas y seguras entre clientes, incluyendo Gibberbot, ChatSecure, Jitsi, y Pidgin. Gibberbot puede añadir una capa para el anonimato y proteger tus comunicaciones de muchas formas de vigilancia en internet ya que se conecta con Orbot.
11. TextSecure
TextSecure es una aplicación para plataformas móviles de Android que encripta mensajes de texto (SMS) a la hora de su envío o mientras están en tu teléfono.
NOTA: Para instalar, configurar y utilizar estas herramientas (casi todas) encontraréis información al respecto en la página web del colectivo Security in-a-box.
https://securityinabox.org/es/seguridadportatil



LA BUSTA
ESPLOSIVA
linguetta isolante
che scorre al momento
dell'apertura
molletta
da bucato
di legno
cavo collegato
ad un polo
della batteria
cavo
collegato
alla
lampadina
lampadina
a basso voltaggio
senza vetro
SACCHETTO
DI ESPLOSIVO
cavo collegato
ad un polo
della batteria
batteria
da 9 v

ILLEGALISMO EGOICO CRIPTATO

